EXHIBIT 3

Chrome Privacy

The Incognito Story

Author: rhalavati@
Status: WIP
Last Update: 2020-02-10

Incognito and Cookies

Websites need to keep data about you, to be able to customize their services to you.

On websites that you sign-in, the websites can keep this data on their own servers, so after you sign-in and tell them who you are, they will fetch the data and continue giving you services based on that. Like when you sign into your social media and see your own page.

But on websites that you don't sign-in, they keep this data locally and on your computer and the next time you visit the website, they use it from there. Like if you go to a train booking website and enter a source and destination to check for tickets, the website may save this data on your computer and next time you visit it, it will give you a faster service for this possible trip. A generic name for this data that websites store on your computer is cookie. Even websites that you sign into them may sometimes store cookies on your computer, to give you faster services next time you return, or keep you signed in.

Incognito mode comes in handy, when you don't want this information to be available to a website. Whenever you open an incognito session (read more about what session is in the next section), your browsing experience starts with an empty cookie jar, therefore the websites will not have any memory of what you have done before.

For example if you have logged into a website in your regular profile, and you want to experience the website without log-in, you can open an incognito window and go to the website there.

Incognito mode keeps the cookies that websites write in a separate jar (from that of your regular browsing session), and throws them all away whenever you close all your incognito windows.

Incognito windows talk to each other

Sometimes more than one window is more convenient to do a task, like when you are comparing two products on a website, to decide which one you like more. To make this possible, incognito windows that you have open at the same

Commented [1]: Thanks for sharing Ramin! If I might ask, what is the purpose of this doc and who is the audience?

+rorymcclelland@google.com

Commented [2]: This document was originally written as my idea about what a privacy tour about incognito mode should tell. The privacy tour took a different turn, so now this is not planned for any specific audience. I just added you to that comment since we were discussing the same issue in a parallel thread.

Commented [3]: I'm wondering how incognito does this and how the empty cookie jar propagates to these websites, given the statement below: "While Chrome does not keep history of what you do in incognito, the websites can keep a record of them on their own servers and remember it later, or remember whatever you enter in their forms."

Commented [4]: Incognito mode always starts with an empty cookie jar, and throws all cookies away when the last window is closed, therefore websites cannot keep anything local based on incognito browsing. But server side, they can store all user navigations in their site and entered data in forms. This data is not necessarily connected to this certain user (unless they sign-in), but exists.
Like if you go to a search engine in incognito and search for "How to make a bomb", the search engine necessarily does not know your identity, but can remember that someone (from this IP) has searched for how to build a bomb.

Commented [5]: Right. And the website can assign any static identifiers it wants to that user, right?

Commented [6]: By "Static", do you mean persistent through next browsing experience?

Commented [7]: Yes, an identifier assigned to that "user" across multiple visits of that website (using the same IP). Maybe what's missing here is a bridge between IP address and non-cookie website tracking. Incognito doesn't mask IP address, so websites can still track activity to the same user when they access the site, as you said in this sentence: "incognito mode cannot hide that as well from websites..." Since IP addresses are often household-level, I feel we may be glossing over this point, and users may feel we are overindexing on the cookie issue as a redirection.

While not completely perfect, and since websites talk to each other, it seems likely in the user's mind that t ... [1]

Commented [8]: +rorymcclelland@google.com, +sammit@google.com

IP can be used to join the authenticated and incognito sessions and we have a parallel effort to reduce this in incognito mode. ... [2]

Commented [9]: +1 Thanks, Ramin.

Commented [10]: Makes sense on the IP part. I guess I would just say that "combining IP with other data" can be trivial when it comes to things like your user agent, the plugins/extensions you have installed, etc. That data is readily available to any webserver. ... [3]

time share data with each other. Therefore if you have some incognito window open, and sign-in to a website, and open another one when the previous one is still open, the second one is also signed-in.

An entirely clean incognito session starts when you open an incognito window and there is no other incognito window open. And the session ends when you close your last incognito window.

Incognito and History

To give you a more personalized experience, Chrome keeps a history of the websites you visit. This data helps Chrome give you suggestions as you type in, give you better search results, gives you faster browsing experience, and more.

If you want to visit a website and you don't want it to be kept in your history, you can visit it in incognito mode. In incognito mode, the browser does not keep your visited websites and will forget all about them when you close all incognito windows and tabs.

You should note that this promise does not apply to what the websites that you visit do. While Chrome does not keep history of what you do in incognito, the websites can keep a record of them on their own servers and remember it later, or remember whatever you enter in their forms. This becomes more serious if you login to the website, read more in the next section!

Incognito and Identity

When you open a new incognito session, any website that you visit will see you as a new user and won't know who you are. But if you tell them who you are, like by signing-in with your username and password, they will know and they can keep track of your activities from that moment on. It's like when you wear a mask, but you introduce yourself to the others. Incognito mode cannot keep your identity secret in these cases, because you have clearly and directly given that to the websites.

Incognito helps you fill forms, but doesn't keep anything

When you browse incognito, you have access to all your saved data in Chrome, such as addresses, credit cards, passwords, etc for more convenience. But to make sure Chrome does not keep any trace of your activities, if you enter a new address, or a credit card, or a password, Chrome will not save it for you. So incognito has access to your data, but cannot change it.

Incognito can also use the history that Chrome has recorded from you to provide suggestions while you type, or autocompletion, but does not contribute to it.

Incognito and Browser Personalization

You can set up your browser to have a more fine-tuned experience. Like if you trust a website to always have access to your camera, you can tell Chrome to always give permission to it. Or you can tell it to always let a certain website show you notifications.

When you go to incognito, all these permissions are ignored and all websites are treated as privately as when you have a new browser. An exception to this is when you add more restrictions for a website, like when you tell Chrome to never let a website access your camera. In this case, incognito will also apply the more restricted preference.

Another exception to personalization reset is bookmarks. For convenience in accessing your frequently used websites, your bookmarks are available in incognito mode, and if you add a bookmark in incognito mode, it will stay there even when you close incognito.

Incognito and Network and Location

Computers and phones, and therefore browsers, can communicate with the internet only through your local network (school, work, or whoever runs the network that you are using). Therefore all your browsing experience, regardless of being incognito or not, will be partly visible by this network, and incognito mode cannot do anything with respect to hiding your data from the network.

Also you must note that websites can guess where you (roughly) are based on your network address (IP), incognito mode cannot hide that as well from the websites.

Incognito and Ads

Tired of ads following you, well, Incognito prevents ads from following you but there are some limits. When you start a new incognito session, all the advertisers will see you as a new person. So any ad that has been following you before, would have a hard time follow you in incognito mode[1]. But, advertisers will see you as a new person in incognito mode and until you close your last incognito window, they can follow you based on what they have seen from you in that incognito session. This advantage is bilateral, the advertisers in websites that you are visiting in regular mode also don't know about your activity in incognito mode. So if you see an ad in incognito mode, it would be hard for it to follow you in regular mode.

---

[1] Incognito cannot entirely block them, because some advertisers may try to create a fingerprint of your device based on the network and hardware information that they can get from it, and through that even follow you in incognito mode.

Page 1: [1] Commented [7] **Ben Kamber** **2/10/2020 7:11:00 AM**

Yes, an identifier assigned to that "user" across multiple visits of that website (using the same IP). Maybe what's missing here is a bridge between IP address and non-cookie website tracking. Incognito doesn't mask IP address, so websites can still track activity to the same user when they access the site, as you said in this sentence: "incognito mode cannot hide that as well from websites..." Since IP addresses are often household-level, I feel we may be glossing over this point, and users may feel we are overindexing on the cookie issue as a redirection.

While not completely perfect, and since websites talk to each other, it seems likely in the user's mind that there are lookup services - educated guesses that IP address x.y.z.zz is Ben Kamber based on my other traffic and authenticated Google searches. Couldn't IP (as imperfect and coarse as it is) then serve as a join key to link my incognito searches (which websites may discern given a lack of cookies) and authenticated searches? Apologies if this is a very obvious issue or if I'm misunderstanding.

Page 1: [2] Commented [8] **Ramin Halavati** **2/10/2020 7:33:00 AM**

+rorymcclelland@google.com, +sammit@google.com

IP can be used to join the authenticated and incognito sessions and we have a parallel effort to reduce this in incognito mode.
But _as far as I know_ IP is not a trustable unique identifier and that's why some websites try to combine it with other fingerprinting approaches to create a stable detection method across signed-out visits and clearing browsing data.
Therefore generally we can say that websites do not know who you are in incognito mode, but they can guess if they keep enough data.

Page 1: [3] Commented [10] **Sammit Adhya** **2/16/2020 1:45:00 AM**

Makes sense on the IP part. I guess I would just say that "combining IP with other data" can be trivial when it comes to things like your user agent, the plugins/extensions you have installed, etc. That data is readily available to any webserver.

IANAL, but from a legal perspective, we would never said that Google doesn't know who you are while you're Incognito, and I think saying websites don't know who you are is potentially misleading until you add all the caveats (e.g. you don't sign in, you close the browser, and somehow prevent the fingerprinting techniques to happen). The only promise we can make today is one about local privacy.

Excited to be heading in that direction though so we can potentially make some stronger promises!